ABSTRACT OF THE DISCLOSURE

Providing an encryption scheme which is invulnerable to the low-density attack based on the LLL algorithm and capable of improving the security. Ciphertext is obtained by a product-sum operation of the components of a composite vector, which is obtained by adding a random number vector whose components are arbitrarily selected random numbers to a plaintext vector obtained by dividing plaintext to be encrypted, and the components of a public-key vector modulo-transformed based on one or a plurality of base vectors which are set such that $V_i = (d/d_i)\cdot v_i$ (where $d = d_1 d_2 \ldots d_K$) by using one or a plurality of sets of integers d_i $(1 \leqq i \leqq K)$. The positions of the components of the plaintext vector or random number vector in the composite vector are arbitrarily set by an entity as the sender or an entity as the receiver.